# Authentication Formats for UAS

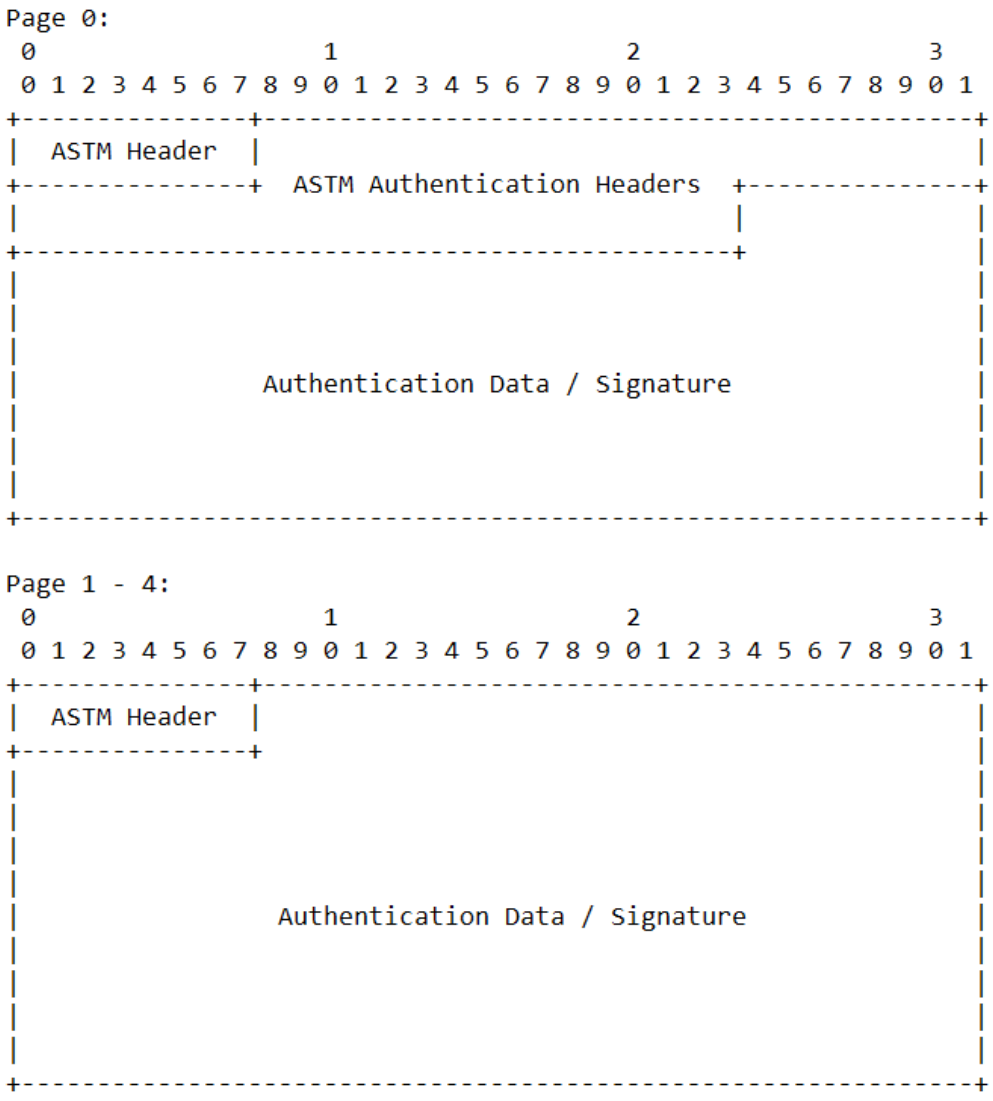
draft-wiethuechter-tmrid-auth-03

Adam Wiethuechter

TMRID BOF – IETF 106 - November 19th, 2019

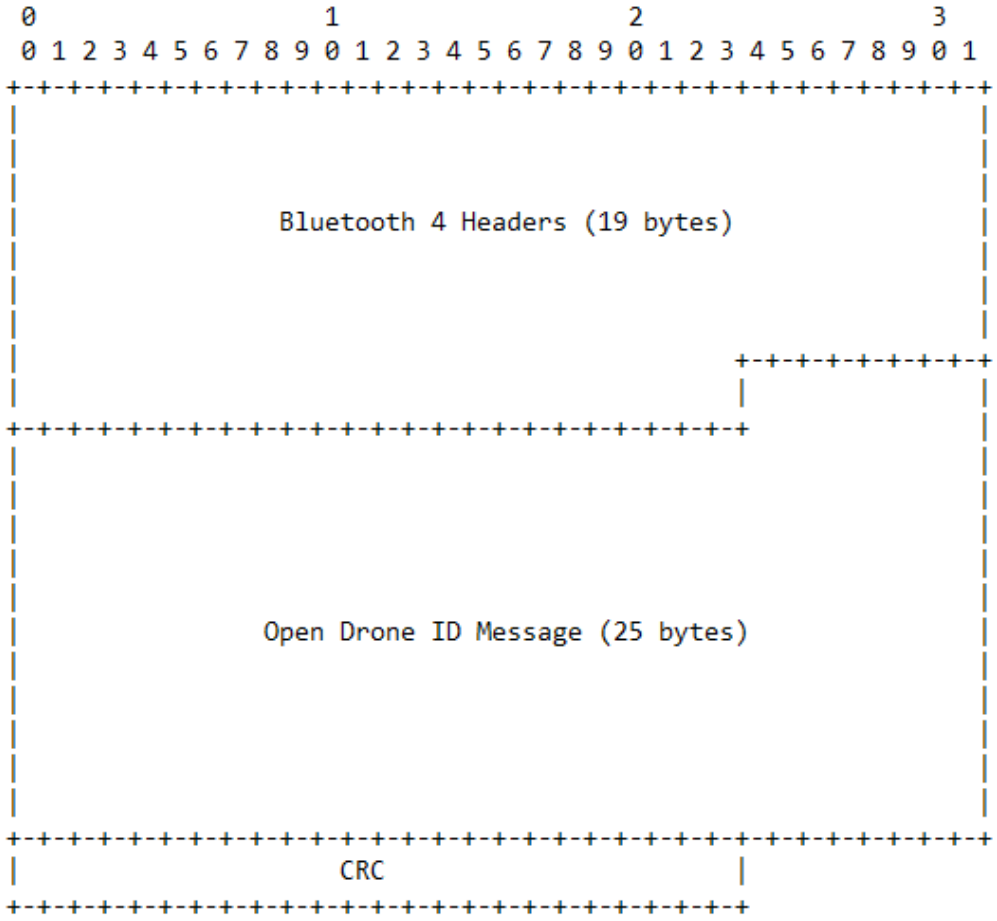
# Background

- ASTM Standard from F38 Committee
  - WK65041: New Specification for UAS Remote ID and Tracking
  - Passed ballot Nov 7th, will become available soon
- Authentication message
  - 5 pages long with a 109 byte max payload (17 + 23 * 4)
  - Design driven to authenticate atomic message and carry certs



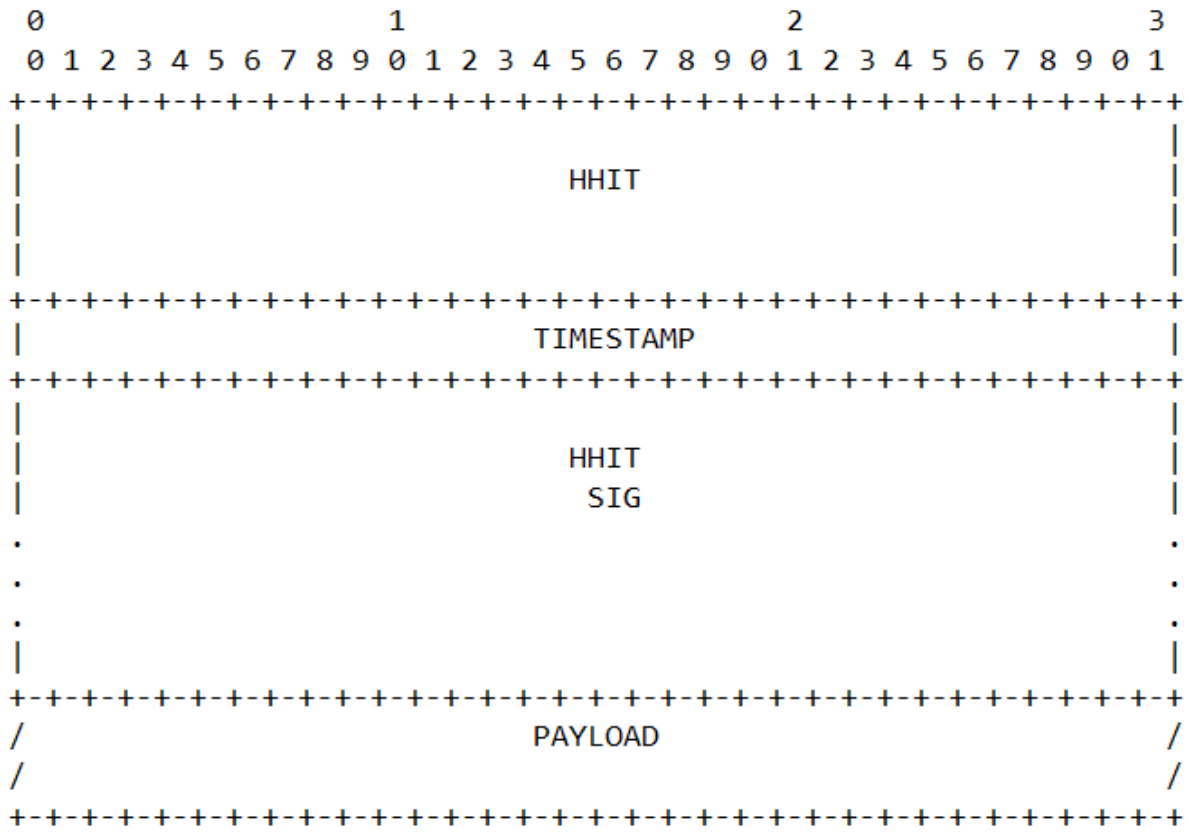
# Bluetooth Background

- Why so small?
  - Bluetooth 4 legacy frames only give 25 bytes to play with (after Bluetooth headers)
  - 1 byte is for a main header in Open Drone ID (ODID) that is always present – now only 24 bytes
  - Auth message has its own header + other fields



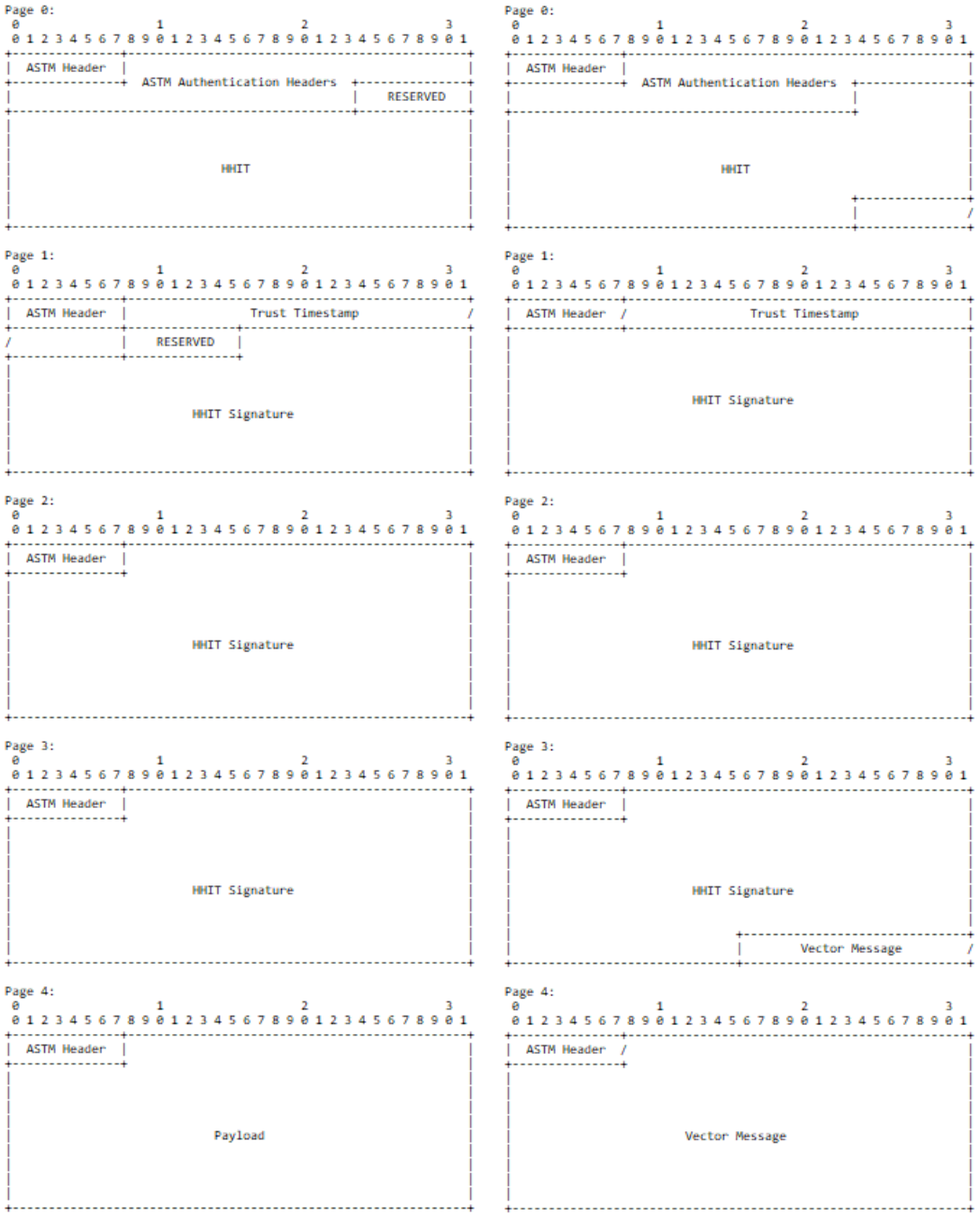
# HIP Based Authentication Wrapper

- HHIT can be looked up to obtain HI from DNS, thus allowing verification of HHIT being genuine
- Payload is used to generate Signature
  - Must have some sort of dynamic field in data to be signed, Trust Timestamp could be used for this if Payload static
- Signature can be verified using HI + Auth message fields



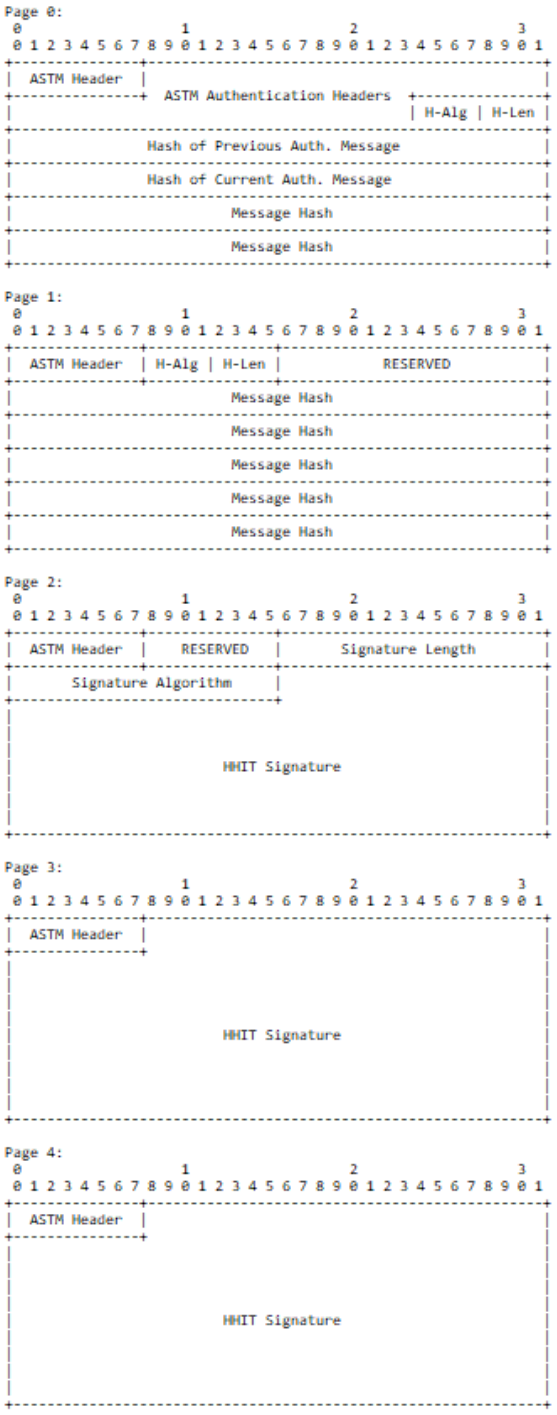
# Trusted [Vector] Message

- Base format (left image)
- An example using Vector message (right image)
  - Vectors are dynamic so at minimum just the 25 byte Payload needs to be signed
- Prototype of format developed at AX Enterprize
  - Currently only the send side of operation with manual verification test



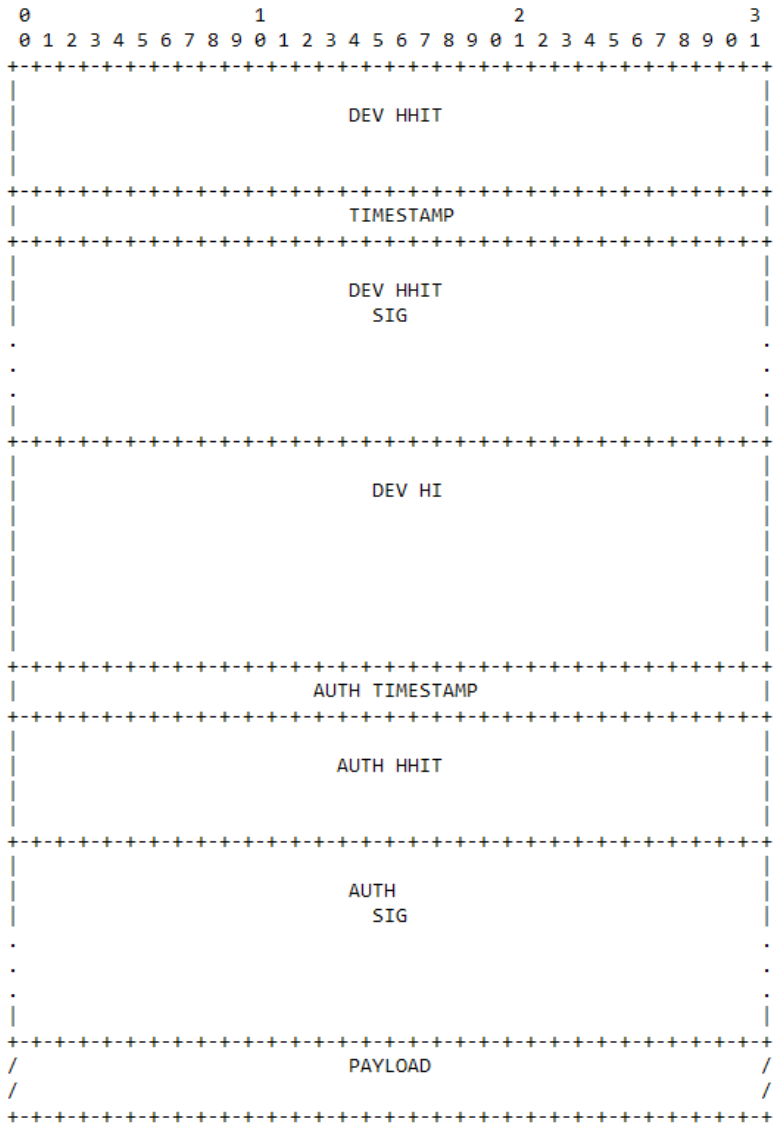
# Signed Hash Lists

- Provides provenance to previously sent messages (left image)
  - Agility through H-Alg and H-Len fields
  - Pseudo-blockchain hashes to link signed lists together
- Could also use idea in wrapper format (right image)
  - Removes pseudo-blockchain hashes, lowers count
- Is the number of hashes worth it?




# HIP Based Offline Authentication

- Currently unobtainable with ASTM format
  - Need at least 10 pages, not 5 pages
- DEV side
  - HHIT and Signature validation can be done without any lookups
- AUTH side
  - Registry HHIT and SIG to show, without lookup, the registry UA belongs in
  - Local cached list of Registries on Observer device
  - Trust can be asserted from information if desired
- Further lookups and validation once connectivity restored for Observer

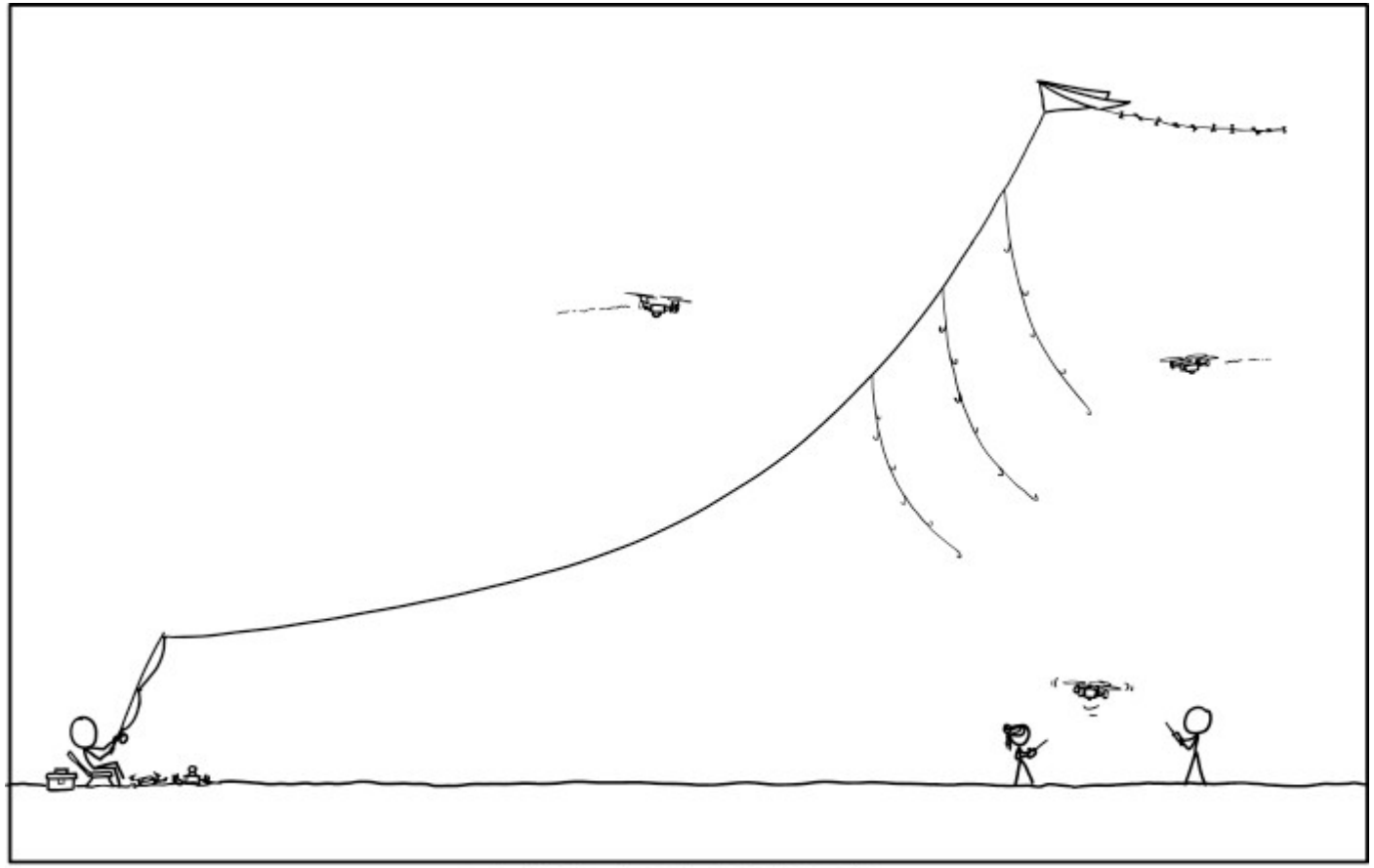


# Future Work Needed

- Work with ASTM on expanding 5 pages to 10 pages
  - Format might migrate into ASTM instead of staying in IETF
- Format; improvements?
- Draft work
  - Security/IANA Considerations
  - Missing prose anywhere?
- Development of prototypes
  - Wrapper Message (receive side)
  - Signed Hash Lists

# Q&A

Questions, Comments, Concerns?




“Today's consumers who order their drones off the internet don’t know the joy of going out in nature and returning with a drone that you caught yourself, whose angry owners you fought off with your own two hands.”
https://xkcd.com/2208/

# Backup Slides

# BT4 Single & Multi packet